IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	**Eugene Amdur, et al.**	Art Unit **2134**
Serial No.:	**09/614,487**	
Confirm. No.:	**2054**	
Filed:	**July 11, 2000**	Primary Examiner **David Yiuk Jung**
For:	**Generation and Use of Digital Signatures**	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS PURSUANT TO 37 C.F.R. § 41.37

Sir:

The Appellants hereby submit their Appeal Brief pursuant to 37 C.F.R. § 41.37 concerning the above-referenced Application.

(i) REAL PARTY IN INTEREST

The Assignee of all right, title and interest to the above-referenced Application is Hewlett-Packard (Canada) Co., a Canadian corporation.

(ii) RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and the Assignee of the present application are not aware of any prior or pending appeals, interferences or judicial proceedings which may be related to, directly affect or have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF CLAIMS

Claims 11-16 are pending in the Application.

Claims rejected:	11-16
Claims allowed:	none
Claims confirmed:	none
Claims withdrawn:	none
Claims objected to:	none
Claims canceled:	1-10

Appellants appeal the rejections of claims 11-16. These claim rejections were the only claim rejections present in the Office Action ("Final Action") dated July 26, 2005, which was Final.

(iv) STATUS OF AMENDMENTS

A Final rejection was made July 26, 2005. No amendments to the claims were requested to be admitted after the non-final rejection.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

Concise explanations of exemplary forms of the claimed invention:

With respect to independent claim 11

An exemplary form of the invention is directed to a computer program product for use with a client-server computer network (Figure 2; Page 5, line 1, to page 6, line 12; Page 9, line 7, to page 11, line 9). The network comprises a set of server computers (30, 32, 34) and a set of client computers (36). The computer program product comprises a computer usable medium having computer readable program code embodied in said medium for providing authentication of cookies.

The computer program product comprises a computer readable program code operative to enable one or more of the set of client computers to provide client-identifying data to one or more of the set of server computers (Page 5, lines 8-9). In addition, the computer program product comprises computer readable program code operative to provide a unique server-identifier for each one of the set of server computers (Page 10, lines 18-20). Also, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to request a private key (40) and an associated public key (42, 44, 46) from a public key encryption system (Page 5, lines 10-12). Further, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to store the requested private key in a dynamic memory device on the server computer, only (Page 5, lines 13-14; Page 10, line 21). In addition, the computer program product comprises computer readable program code operative to enable each one of the set of

server computers to store the requested public key in a database (38) available to the set of server computers (Page 5, lines 15-17), and to associate the stored public key requested by the server computer with the unique server-identifier for the server computer (Page 11, line 3-4). Further, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to generate cookies for one or more of the set of client computers (Page 5, lines 18-20). Each generated cookie comprises data corresponding to the client-identifying data provided by the one or more of the set of client computers (Page 5, lines 20-21) and comprising the value of the server-identifier assigned to the generating server (Page 11, lines 1-2). Also, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to generate an encrypted digital signature for each generated cookie using the requested private key stored in dynamic memory on the server computer (Page 5, lines 22-26; Page 10, lines 13-16). Further, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to forward cookies and their associated encrypted digital signatures to the client computers corresponding to the identifying data provided (Page 5, lines 27-29). In addition, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to receive cookies with encrypted digital signatures from one or more of the set of client computers (Page 6, lines 1-5). Further, the computer program product comprises computer readable program code operative to enable each one of the set of server computers to extract server-identifying data from received cookies to retrieve associated public keys from the database for use in decrypting digital signatures for received cookies and thereby to authenticate the said cookies (Page 6, lines 6-12; Page 11, lines 1-9).

With respect to independent claim 14

Another exemplary form of the invention is directed to a method for providing authentication of cookies in a client-server computer network (Figure 2; Page 6, line 14, to page 7, line 17; Page 9, line 7, to page 11, line 9). The network comprises a set of server computers (30, 32, 34) and a set of client computers (36). Each one of the set of server computers has a unique server-identifier (Page 10, lines 18-20). The method comprising a first one of the set of client computers providing client-identifying data to a first one of the set of server computers (Page 6, lines 17-19). The method also comprises the first one of the set of server computers requesting a private key (40) and an associated public key (42, 44, 46) from a public key encryption system (Page 6, lines 20-21). In addition, the method comprises the first one of the set of server computers storing the requested private key in a dynamic memory device, on the first server computer, only (Page 6, lines 22-23; Page 10, line 21). The method further comprises the first one of the set of server computers causing the requested public key to be stored in a database (38) available to each one of the set of server computers (Page 6, lines 24-25); and to associate the stored public key with the unique server-identifier for the first one of the set of server computers (Page 11, line 3-4). Also, the method comprises the first one of the set of server computers generating a cookie for the first one of the set of client computers (Page 6, lines 26-27). The cookie comprises data corresponding to the client-identifying data provided by the first one of the set of client computers (Page 6, lines 27-28), and comprises the value of the server-identifier for the first one of the set of server computers (Page 11, lines 1-2). The method also comprises the first one of the set of server computers generating an encrypted digital signature for the cookie using the private key stored in dynamic memory of the first one of the set

of server computers (Page 7, lines 3-4; Page 10, lines 13-16). In addition, the method comprises the first one of the set of server computers forwarding the cookie including the associated encrypted digital signature to the first one of the set of client computers (Page 7, lines 5-7). Further, the method comprises the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie including the encrypted digital signature from the first one of the set of client computers (Page 7, lines 8-11). The method also comprises the second one of the set of server computers extracting server-identifying data from the received cookie to retrieve the associated public key for the encrypted digital signature from the database for use in decrypting the digital signature for the received cookie and thereby authenticating the cookie (Page 7, lines 12-17; Page 11, lines 1-9).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds to be reviewed in this appeal are:

Whether Appellants' claim 11 is unpatentable under 35 U.S.C. § 102(b) over Mitsutaka Kikuchi, et al., Japanese Patent #11-98134-A ("Kikuchi");

Whether Appellants' claim 12 is unpatentable under 35 U.S.C. § 103(a) over Kikuchi;

Whether Appellants' claims 13 is unpatentable under 35 U.S.C. § 103(a) over Kikuchi in view of Bruce Schneier, "Applied Cryptography" ("Schneier"); and

Whether Appellants' claims 14, 15, and 16 are unpatentable under 35 U.S.C. § 103(a) over Kikuchi in view of Schneier and in further view of Devine et al., U.S. Patent No. 6,606,708 ("Devine").

Additional Comment.

The statutory bases for the Rejections of claims 11-16 were not explicitly stated in the Final Action dated July 26, 2005. Rather, the Final Action stated that the claim rejections can be found in the earlier Office Action dated January 4, 2005 ("earlier Action"). Although the Examiner's clarification (on page 3) of the errors found in the earlier Action was helpful in reconstructing the intended rejections, the absence of a written statement of the statuary basis for the rejections of claims 11-16 in the Final Action leaves room for error. Thus if the above list of

grounds of rejection to be reviewed on appeal does not accurately mirror each of the rejections intended to be made by the Examiner, Appellants' reserve the right to present additional grounds to be reviewed on appeal in a future Reply Brief.

(vii) ARGUMENT

Kikuchi Reference

The Kikuchi reference is directed to a WWW computer (1) that sends a digitally signed cookie (3) to a client (2). The same WWW computer (1) is then capable of receiving the cookie (3) and authenticating the cookie (Figure 1).

Schneier Reference

The Schneier reference corresponds to selected pages of a book directed to cryptography.

Devine, US Patent No. 6,606.708

The Devine reference is directed to a double firewalled system. The system includes a load balancer to distribute a session connection load among a high number of authorized client users (Abstract). The system includes session data/cookie mapping to provide the identity of the user and any other "session-related information". (Figure 4; Column 14, lines 6-10). Devine specifically teaches that the cookies are generated by a "cookie jar" server (32) which is sent to the client. Devine also specifically teaches that such a separate "cookie jar" server (32) is desirable to minimize the load on the dispatch server (26) (Column 8, lines 50-60).

The 35 U.S.C. § 102 (b) Rejections

The Applicable Legal Standards

Anticipation pursuant to 35 U.S.C. § 102 requires that a single prior art reference contain all the elements of the claimed invention arranged in the manner recited in the claim. *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

Anticipation under 35 U.S.C. § 102 requires, in a single prior art disclosure, each and every element of the claimed invention arranged in a manner such that the reference would literally infringe the claims at issue if made later in time. *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747, 3 USPQ2d 1766, 1768 (Fed. Cir. 1987).

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency, the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999).

It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

Rejection under 35 U.S.C. § 102(b) over Kikuchi

Claim 11 was rejected under 35 U.S.C. § 102(b) as being anticipated by Kikuchi. This rejection is respectfully traversed.

Claim 11

Claim 11 is an independent claim directed to a computer program product for use with a client-server computer network. Appellants respectfully submit that Kikuchi does not disclose each feature and relationship recited in claim 11.

As discussed previously, the Final Action dated July 26, 2005 did not explicitly state the statutory basis and reasons for the rejection of claim 11. Rather, the Final Action referred to the earlier Action dated January 4, 2005. Therefore the arguments presented herein refer to both the Final Action and the earlier Action to explain the reasoning behind why the presumed rejections are improper and should be withdrawn.

In the earlier Action, the Examiner states that, "Unique server identifier for each of server computers/www service adds digital signature to Cookie (Section 6, lines 3, '134)". Appellants presume this statement is intended to show where element "b." in claim 11 is found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in element "b." in claim 11. For example, element "b." in claim 11 recites:

> b. computer readable program code operative to provide a unique server-identifier for each one of the set of server computers.

However, Section 6, line 3, in Kikuchi only discuses adding a digital signature to a cookie. Although a digital signature may be used to authenticate the cookie, Kikuchi does not disclose or suggest that such a digital signature is capable of corresponding to the recited unique server-identifier for a server computer. In addition, it would not be inherent that digital signatures include or correspond to unique identifiers.

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency, the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999). A digital signature, for example, may correspond to an encrypted hash of the message being digitally signed. However, Kikuchi does not disclose or suggest that a digital signature is used as a unique identifier of a server. Further, as a digital signature will have a value that changes depending on the content of the message, a digital signature does not have characteristics which would suggest it would be useful to serve as a unique identifier for a server. Thus a unique identifier of a server is not "necessarily present" or associated with the digital signature described in Kikuchi. It follows that Kikuchi does not disclose or suggest element "b." of claim 11.

In the earlier Action, the Examiner wrote, "Request/Store public/private key from public key encryption system. . . / Efficient digital signature scheme (Section 19, Line 1, '134)".

Appellants presume that this statement is intended to show where elements "c." and "d." in claim 11 are found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in elements "c." and "d." in claim 11. For example, element "c." in claim 11 recites:

> c. computer readable program code operative to enable each one of the set of server computers to request a private key and an associated public key from a public key encryption system.

Section 19, line 1 of Kikuchi discuses an ESIGN "Efficient digital Signature Scheme". However, Kikuchi only states that the ESIGN is "used for creation and verification of digital signature of this Cookie". Kikuchi does not disclose or suggest that an ESIGN is operative to perform the recited feature of enabling each one of a set of server computers to request a private key and an associated public key from a public key encryption system. In addition, Kikuchi also does not disclose or suggest that the ESIGN is operative to return a private key and an associated public key to one of the set of server computers. The mere statement that the ESIGN is used for creation and verification of digital signature of this Cookie also does not inherently require the recited features. For example, the ESIGN could include the necessary encryption keys itself to carry out creation and verification and therefore would not need to request both a public and private key from a public key encryption system and/or would not need to return both a public and private key to a server. Thus Kikuchi does not disclose or suggest element "c." of claim 11.

In addition, element "d." in claim 11 recites:

d. computer readable program code operative to enable each one of the set of server computers to store the requested private key in a dynamic memory device on the server computer, only.

However, nowhere does Kikuchi disclose or suggest that ESIGN is operative to enable each one of the set of server computers to store the requested private key on the server. Further, nowhere does Kikuchi disclose or suggest that ESIGN is operative to enable each one of the set of server computers to store the requested private key in dynamic memory on the server, only. Thus Kikuchi does not disclose or suggest element "d." of claim 11.

In the earlier Action, the Examiner wrote, "Public key in database available to server computers and associate public key with unique server-identifier / public key must be available to server to validate digital signature, unique server-identifier (private key) is associated with public key by private/public key encryption/decryption relationship". Appellants presume that this statement is intended to show where element "e." in claim 11 is found in Kikuchi. However, Appellants disagree that this statement accurately reflects the teachings of Kikuchi with respect to the features and relationships recited in element "e." in claim 11. For example, element "e." in claim 11 recites:

e. computer readable program code operative to enable each one of the set of server computers to store the requested public key in a database available to the set of

server computers, and to associate the stored public key requested by the server computer with the unique server-identifier for the server computer.

Nowhere does Kikuchi disclose or suggest that each one of a set of server computers is enabled to store a requested public key in a database available to the set of server computes. In addition, nowhere does Kikuchi disclose or suggest associating the stored public key requested by the server computer with the unique server-identifier for the server computer as recited in element "b."

The Action's statement included the phrase "private key" in parenthesis adjacent the recited term of unique server-identifier. Appellants presume that this portion of the earlier Action is now arguing that a private key in Kikuchi corresponds to the recited unique server-identifier. However, the recited private key associated with the recited public key cannot server as the unique identifier. This is because element "d." specifically recites that the private key is stored in a dynamic memory device on the server computer, only, and therefore cannot be available to be stored in association with the public key in a database accessible to the set of server computers as recited in element "e.".

In addition, the earlier Action admits on Page 8 with respect to claim 14 that Kikuchi "does not specifically teach the use of multiple servers where the public key is stored in a database available to each one of the server computers." Thus, as explained above and as admitted in the earlier Action, Kikuchi does not disclose or suggest element "e." of claim 11.

In the earlier Action, the Examiner wrote, "Server computers generate cookies for client computers / Cookie generation part at WWW service computer (Fig 1, Element 13, '134) . . .

Cookie comprises value of server-identifier assigned to the generating server / Adding digital signature to cookie (Section 6, Line 4 et seq., '134)". Appellants presume that these statements are intended to show where at least element "f." in claim 11 is found in Kikuchi. However, Appellants disagree that these referenced portions of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in element "f." in claim 11. For example, element "f." in claim 11 recites:

> f. computer readable program code operative to enable each one of the set of server computers to generate cookies for one or more of the set of client computers, each generated cookie comprising data corresponding to the client-identifying data provided by the one or more of the set of client computers and comprising the value of the server-identifier assigned to the generating server.

Although Kikuchi shows a Cookie Generation part (13) on the computer (1) which provides the WWW service, nowhere does Kikuchi disclose or suggest that the generated cookie (3) comprises the recited feature of the value of the server-identifier assigned to the generating server. Further, as discussed previously, to support the rejection of claim 11, the earlier Action appears to have argued that a private key in Kikuchi corresponds to the server-identifier. However, such an argument would result in a private key being in the cookies generated by Kikuchi and sent to a client – which would not only be highly insecure, but would also contradict yet again element "d." which specifically recites that the private key is stored in a dynamic memory device on the server computer, only. Also, as discussed previously, the earlier Action

also appeared to regard the digital signature as corresponding to the server identifier as well as a digital signature. However, claim 11 recites that the cookie has both the value of the server-identifier (element "f.") and a digital signature (element "h."). The recited server-identifier and the recited digital signature are therefore not the same element. It follows that neither a private key nor or a digital signature in Kikuchi is sufficient to show that Kikuchi discloses or suggests each of the recited features in element "f."

In the earlier Action, the Examiner wrote, "Server computers receive cookies with encrypted digital signatures from client computers / User terminal transmits encrypted message and digital signature to WWW service computer (Fig 2, '134)". Appellants presume that this statement is intended to show where element "i." in claim 11 is found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in element "i." in claim 11. For example, element "i." in claim 11 recites:

> i. computer readable program code operative to enable each one of the set of server computers to receive cookies with encrypted digital signatures from one or more of the set of client computers.

Kikuchi only shows the cookie being returned to the same WWW service computer (1) which originally sent the cookie. Nowhere does Kikuchi disclose or suggest sending cookies with digital signatures from the client to another WWW service computer. Thus nowhere does Kikuchi disclose or suggest the recited feature that each one of the set of server computers is

enabled to receive cookies with encrypted digital signatures from one or more of the set of client computers. Thus Kikuchi does not disclose or suggest element "i." of claim 11.

In the earlier Action, the Examiner wrote, "Servers extract server identifying data from received cookies to retrieve public keys to decrypt digital signatures and authenticate the cookies / Cookie verification part (Section 13, Line 6, '134)". Appellants presume that this statement is intended to show where element "j." in claim 11 is found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in element "j." in claim 11. For example, element "j." in claim 11 recites:

> j. computer readable program code operative to enable each one of the set of server computers to extract server-identifying data from received cookies to retrieve associated public keys from the database for use in decrypting digital signatures for received cookies and thereby to authenticate the said cookies.

Section 13, of Kikuchi discusses a Cookie verification part (14) which verifies whether there is alteration of the cookie. Section 13 also discusses a signature creation and verification part (15) which makes and verifies digital signatures for the cookies. However, again the verification parts (14, 15) are located on the same server (1) which created and sent the cookie to the client. Nowhere does Kikuchi disclose or suggest that a different WWW server other than the one that generated the cookie is operative to decrypt digital signatures for received cookies. Further, nowhere does Kikuchi disclose or suggest the recited infrastructure that would even make this

possible. For example, as explained previously, the cookies of Kikuchi do not include server-identifying data. Thus Kikuchi is not capable of extracting server-identifying data from received cookies, so as to be able to retrieve associated public keys from the database for use in decrypting digital signatures for received cookies. Kikuchi does not disclose or suggest a system that is capable of having a server authenticate a cookies generated by another server. Thus Kikuchi does not disclose or suggest element "j." of claim 11.

In addition, the earlier Action admits on Page 8 with respect to claim 14 that Kikuchi "as modified above does not teach for the client to access a second server and for the second server to authenticate the client's cookie". Thus as explained above and as admitted in the earlier Action, Kikuchi does not disclose or suggest element "j." of claim 11.

Kikuchi does not explicitly or inherently teach the features and relationships recited in claim 11. For all of these many reasons Kikuchi does not anticipate claim 11. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(b) rejection should be withdrawn. It follows the rejections of claims 12 and 13 which depend from claim 11 should also be withdrawn.

The 35 U.S.C. § 103 (a) Rejections

The Applicable Legal Standards

Before a claim may be rejected on the basis of obviousness pursuant to 35 U.S.C. § 103, the Patent Office bears the burden of establishing that all the recited features and relationships of the claim are known in the prior art. This is known as *prima facie* obviousness. To establish *prima facie* obviousness, it must be shown that all the elements and relationships recited in the claim are known in the prior art. If the Office does not produce a *prima facie* case, then the Appellants are under no obligation to submit evidence of nonobviousness. MPEP § 2142 (Eighth Edition, August 2001; Rev. 2, May 2004).

The evidence of record must teach or suggest the recited features. An assertion of basic knowledge and common sense not based on any evidence in the record lacks substantial evidence support. *In re Zurko*, 258 F.3d 1379, 59 USPQ2d 1693 (Fed. Cir. 2001).

Even if all of the features recited in the claim are known in the prior art, it is still not proper to reject a claim on the basis of obviousness unless there is a specific teaching, suggestion, or motivation in the prior art to produce the claimed combination. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1561, 1568, 1 USPQ2d 1593 (Fed. Cir. 1987). *In re Newell*, 891 F.2d 899, 901, 902, 13 USPQ2d 1248, 1250 (Fed. Cir. 1989).

The teaching, suggestion, or motivation to combine the features in prior art references must be clearly and particularly identified in such prior art to support a rejection on the basis of obviousness. It is not sufficient to offer a broad range of sources and make conclusory statements. *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

A determination of patentability must be based on evidence of record. *In re Lee*, 277 F.3d 1338, 61 USPQ2d 1430 (Fed. Cir. 2002).

It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

Rejection under 35 U.S.C. § 103(a) over Kikuchi

Claims 12 and was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kikuchi. This rejection is respectfully traversed.

Claim 12

Claim 12 depends from claim 11. The earlier Action admits that Kikuchi does not explicitly teach the recited feature of a "computer readable program code responsive to the restart of a one of the server computers and operative to request a replacement private key and an associated replacement public key". However, the Examiner states that he takes Official notice as to the means to obtain a replacement key after restart. Appellants disagree.

The present evidence of record does not teach or suggest such features. The rejection relies on conclusory statements, not evidence of record. The Action's mere assertions do not constitute the required prior art evidence of record, and thus lack substantial evidence support. The determination of patentability must be based on evidence of record, not on unsubstantiated assertions under the guise of an Official notice (which is the present situation). As the evidence

of record does not support the rejection, the claims should be allowed. *In re Zurko*, supra. *In re Lee*, supra. MPEP § 2144.03.

Nowhere does Kikuchi disclose or suggest a server that ever requests a private key and associated public key. Also, nowhere does Kikuchi disclose or suggest that a private key is only stored on the server in dynamic memory. In addition, nowhere does Kikuchi disclose or suggest storing a public key in a database. Thus, whether or not volatile dynamic memory is well known in the art, nowhere does Kikuchi in view of volatile dynamic memory disclose or suggest a server that is operative to request a replacement private key and an associated replacement public key. In addition, Kikuchi in view of volatile dynamic memory does not disclose or suggest as recited in claim 12, "computer readable program code operative to cause the replacement public key to be stored in the database". The Office has not established *prima facie* obviousness with respect to claim 12, and it is respectfully submitted the rejection should be reversed.

Rejection under 35 U.S.C. § 103(a) over Kikuchi in view of Schneier

Claim 13 and was rejected under 35 U.S.C. § 103(a) as being unpatentable over Kikuchi in view of Schneier. This rejection is respectfully traversed.

Claim 13

Claim 13 depends from claim 12. The Examiner acknowledged in the earlier Action that Kikuchi does not teach the features recited in claim 13. However, the earlier Action states that "it would have been obvious . . . to implement '134 with the key lifecycle strategies as disclosed in Schneier." Appellants disagree.

As discussed previously, Kikuchi does not disclose or suggest storing public keys in a database. Also, Schneier does not provide a teaching, suggestion, or motivation to modify Kikuchi to include the recited database of public keys. Thus one of ordinary skill in the art would not have been motivated to modify Kikuchi to cause the recited feature of "deletion of public keys in the database where such keys have been stored for longer than a predetermined elapsed time", because Kikuchi does not disclose or suggest having such a database. Thus, Appellants respectfully request that the 35 U.S.C. § 103(a) rejection of claim 13 be withdrawn.

Rejection under 35 U.S.C. § 103(a) over Kikuchi in view of Schneier

Claims 14-16 were presumably rejected under 35 U.S.C. § 103(a) as being unpatentable over Kikuchi in view of Schneier and further in view of Devine. These rejections are respectfully traversed.

Claim 14

Claim 14 is an independent claim directed to a method. Appellants respectfully submit that Kikuchi does not disclose each feature, relationship and step recited in claim 14.

As discussed previously, the Final Action dated July 26, 2005 did not explicitly state the statutory basis and reasons for the rejection of claim 14. Rather, the Final Action referred to the earlier Action dated January 4, 2005. Therefore the arguments presented herein refer to both the Final Action and the earlier Action to explain the reasoning behind why the presumed rejections are improper and should be withdrawn.

In the earlier Action, the Examiner wrote, "Unique server identifier for each of server computers/www service adds digital signature to Cookie (Section 6, lines 3, '134)". Appellants presume this statement is intended to show where elements in the preamble of claim 14 are found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in the preamble of claim 14. For example, the preamble of claim 14 recites:

> A method for providing authentication of cookies in a client-server computer network, the network comprising a set of server computers and a set of client computers, each one of the set of server computers having a unique server-identifier.

However, Section 6, line 3 in Kikuchi only discuses adding a digital signature to a Cookie. Although a digital signature may be used to authenticate the Cookie, Kikuchi does not disclose or suggest that such a digital signature is capable of corresponding to the recited unique server-identifier for each one of the set of server computer. In addition, it would not be inherent that digital signatures include or correspond to unique identifiers.

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency, the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used

or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999).

A digital signature, for example, may correspond to an encrypted hash of the message being digitally signed. However, Kikuchi does not disclose or suggest that a digital signature is used as a unique identifier of a server. Further, as a digital signature will have a value that changes depending on the content of the message, a digital signature does not have characteristics which would suggest it would be useful to serve as a unique identifier for a server. Thus a unique identifier of a server is not "necessarily present" or associated with the digital signature described in Kikuchi.

Kikuchi does not disclose or suggest each of the features recited in the preamble of claim 14. In addition, the Action has not shown where either Schneier or Devine discloses or suggests these recited features which are not disclosed or suggested in Kikuchi. Thus the Office has not established *prima facie* obviousness with respect to the features recited in the preamble of claim 14.

In the earlier Action, the Examiner wrote, "Request/Store public/private key from public key encryption system. . . / Efficient digital signature scheme (Section 19, Line 1, '134)". Appellants presume that this statement is intended to show where steps "b." and "c." in claim 14 are found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in steps "b." and "c." in claim 14. For example, step "b." in claim 14 recites:

b. the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system.

Section 19, line 1 of Kikuchi discusses an ESIGN "Efficient digital Signature Scheme". However, Kikuchi only states that the ESIGN is "used for creation and verification of digital signature of this Cookie". Kikuchi does not disclose or suggest that an ESIGN is operative cause a first one of a set of server computers to carry out requesting a private key and an associated public key from a public key encryption system. In addition, Kikuchi also does not disclose or suggest that the ESIGN is operative to return a private key and an associated public key to a first one of the set of server computers. The mere statement that the ESIGN is used for creation and verification of digital signature of this Cookie also does not inherently require the recited features. For example, the ESIGN could include the necessary encryption keys itself to carry out creation and verification and therefore would not need to request both a public and private key from a public key encryption system and/or would not need to return both a public and private key to a server. Thus Kikuchi does not disclose or suggest step "b." of claim 14. In addition, the Actions have not shown where either Schneier or Devine discloses or suggests this step which is not disclosed or suggested in Kikuchi. Thus the Office has not established *prima facie* obviousness with respect to step "b." of claim 14.

In addition, step "c." in claim 14 recites:

c. the first one of the set of server computers storing the requested private key in a dynamic memory device, on the first server computer, only.

However, nowhere does Kikuchi disclose or suggest that ESIGN is operative to cause the server to store the requested private key on the first server computer. Further, nowhere does Kikuchi disclose or suggest that ESIGN is operative to cause the server to store the requested private key in a dynamic memory device, on the first server computer, only. Thus Kikuchi does not disclose or suggest step "c." of claim 14. In addition, the Actions have not shown where either Schneier or Devine discloses or suggests this step which is not disclosed or suggested in Kikuchi. Thus the Office has not established *prima facie* obviousness with respect to step "c." of claim 14.

In the earlier Action, the Examiner wrote, "Public key in database available to server computers and associate public key with unique server-identifier / public key must be available to server to validate digital signature, unique server-identifier (private key) is associated with public key by private/public key encryption/decryption relationship". Appellants presume that this statement is intended to show where step "d." in claim 14 is found in Kikuchi. However, Appellants disagree that this statement accurately reflects the teachings of Kikuchi with respect to the features and relationships recited in step "d." of claim 14. For example, step "d." in claim 14 recites:

> d. the first one of the set of server computers causing the requested public key to be stored in a database available to each one of the set of server computers, and to associate the stored public key with the unique server-identifier for the first one of the set of server computers.

Nowhere does Kikuchi disclose or suggest that its server computer causes the requested public key to be stored in a database available to each one of the set of server computers. In addition,

nowhere does Kikuchi disclose or suggest associating the stored public key requested by the first one of the set of server computers with the unique server-identifier for the first one of the set of server computers. The above statement in the earlier Action included the phrase "private key" in parenthesis adjacent the recited term of unique server-identifier. Appellants presume that this portion of the earlier Action is now arguing that a private key in Kikuchi corresponds to the recited unique server-identifier. However, the recited private key associated with the recited public key cannot server as the unique identifier. This is because step "c." specifically recites that the private key is stored in a dynamic memory device, on the first server computer, only, and therefore cannot be available to be stored in association with the public key in a database accessible to the set of server computers as recited in step "d.". Thus Kikuchi does not disclose or suggest step "d." of claim 14.

In addition, the earlier Action also conceded (at page 8) that Kikuchi "does not specifically teach the use of multiple servers where the public key is stored in a database available to each one of the server computers." However, the earlier Action stated that, "Schneier teaches the use of a centralized public key database for multiple parties to access the public key to a public/private key pair (Page 185, "Public-Key Key Management", Line 3 et seq., Schneier)." The earlier Action then stated that it would have been obvious to a person of ordinary skill in the art at the time of invention to use the centralized public key database taught by Schneier in the invention of client-server system '134. One of ordinary skill in the art would have been motivated to use the centralized public key database taught by Schneier in the invention of client-server system of '134 because the centralized public key database provides a simple scalable public key management system." Appellants disagree.

Although Schneier teaches a centralized database to store public keys, the Office has failed to show where Schneier, Kikuchi, or Devine teach or suggest the recited feature in step "d." of "associate the stored public key with the unique server-identifier for the first one of the set of server computers". Thus the Actions have not established *prima facie* obviousness with respect to step "d." of claim 14. In addition, the Actions have not shown a prior art teaching, suggestion or motivation to modify Kikuchi to include a centralized public key database. For example, where in Kikuchi is it suggested that there is a need for the asserted "scalable public key management system for the cookie generating system of Kikuchi. Also, where in either Schneier or Devine is it suggests that a cookie generating system such as Kikuchi could use a centralized database to store public keys?

In addition, the system of Kikuchi teaches a system that requires the same server to authenticate the cookie originally generated by that server. Thus there is no motivation in Kikuchi to place public keys in a centralized database, as only one server would ever need to retrieve the public key from the database for that one server. Kikuchi does not provide any motivation for more than one server to access the same public key. Consequently it would not be obvious to modify Kikuchi with the teachings of Schneier as suggested. Therefore step "d." would not be obvious in view of the applied art.

In the earlier Action, the Examiner wrote, "Server computers generate cookies for client computers / Cookie generation part at WWW service computer (Fig 1, Element 13, '134) . . . Cookie comprises value of server-identifier assigned to the generating server / Adding digital signature to cookie (Section 6, Line 4 et seq., '134)". Appellants presume that these statements are intended to show where at least step "e." in claim 14 is found in Kikuchi. However, Appellants disagree that these referenced portions of Kikuchi or any other portion of Kikuchi

shows each and every feature and relationship recited in step "e." in claim 14. For example, step "e." in claim 14 recites:

> e. the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the client-identifying data provided by the first one of the set of client computers, and comprising the value of the server-identifier for the first one of the set of server computers.

Although Kikuchi shows a Cookie Generation part (13) on the computer (1) which provides the WWW service, nowhere does Kikuchi disclose or suggest that the cookie generated by a first one of a set of server computers comprises the recited feature of the value of the server-identifier for the first one of the set of server computers. Further, as discussed previously, to support the rejection of claim 14, the earlier Action appears to be arguing that the private key corresponds to the server-identifier. However, such an argument would result in a private key being in the cookies generated by Kikuchi and sent to a client – which would not only be highly insecure, but also would contradict yet again step "c." which specifically recites storing the requested private key in a dynamic memory device, on the first server computer, only. Also as discussed previously, the earlier Action also appeared to regard the digital signature as corresponding to the server identifier as well as a digital signature. However, claim 14 recites that the cookie has both the value of the server-identifier for the first one of the set of server computers (step "e.") and a digital signature (step "g."). The recited server-identifier and the recited digital signature are

therefore not the same element. It follows that neither a private key nor or a digital signature in Kikuchi is sufficient to show that Kikuchi discloses or suggests each of the recited features in step "e."

In addition, the Actions have not shown where either Schneier or Devine discloses or suggests this step (e.g., generating a cookie comprising the value of the server-identifier for the first one of the set of server computers) which is not disclosed or suggested in Kikuchi. Thus the Office has not established *prima facie* obviousness with respect to step "e." of claim 14.

In the earlier Action, the Examiner wrote, "Server computers receive cookies with encrypted digital signatures from client computers / User terminal transmits encrypted message and digital signature to WWW service computer (Fig 2, '134)". Appellants presume that this statement is intended to show where step "h." in claim 14 is found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in step "h." in claim 14. For example, step "h." in claim 14 recites:

> h. the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie including the encrypted digital signature from the first one of the set of client computers.

Kikuchi only shows the cookie being returned to the same WWW service computer (1) which originally sent the cookie. Nowhere does Kikuchi disclose or suggest sending cookies with

digital signatures from the client to another WWW service computer. Thus nowhere does Kikuchi disclose or suggest the recited feature the second one of the set of server computers requesting and receiving the cookie including the encrypted digital signature from the first one of the set of client computers. Thus Kikuchi does not disclose or suggest step "h." of claim 14.

In addition, the earlier Action acknowledged (at page 8) that Kikuchi does not teach for the client to access a second server and for the second server to authenticate the client's cookie. However, the earlier Action stated that Devine "teaches a load balancing system for multiple servers to communicate with a client using authentication cookies (Col 23, Lines 29-33, '708), (Col 8, Lines 46-56, '708)." The earlier Action then states that it "would have been obvious . . . to use the load balanced multiple server system of '708 with the invention of '134 as modified above. One of ordinary skill in the art would have been motivated to use the load balanced multiple server system of '708 with the invention of '134 as modified above because the use of multiple servers allows for faster data communication speeds for a greater number of accessing clients." Appellants disagree.

These referenced portions of Devine do not disclose or suggest the admitted feature missing from Kikuchi of a client that accesses a second server and for the second server to authenticate the client's cookie. Devine specifically teaches that a separate "cookie jar" server 32 which generates cookies is desirable to minimize the load on the dispatch server (26) (Column 8, lines 50-60). Thus by teaching the advantages of a separate "cookie jar" server, Devine specially teaches away from having different WWW servers generate their own cookies. A reference teaching away from the recited invention does not support *prima facie* obviousness. It is improper to reconstruct the invention from the disclosure of the Appellants. An obviousness

rejection cannot be based on a combination of features in references if making the combination would result in destroying the utility or advantage of the device shown in the prior art references. Note *In re Fine 5 USPQ2d 1598-99 (Fed. Cir. 1988).* Therefore Devine does not show a prior art teaching suggestion or motivation to modify Kikuchi as suggest in the earlier Action. Therefore, it would not have been obvious to one having ordinary skill in the art to have modified Kikuchi in view of Schneier and Devine as suggested to carry out step "h."

In the earlier Action, the Examiner wrote, "Servers extract server identifying data from received cookies to retrieve public keys to decrypt digital signatures and authenticate the cookies / Cookie verification part (Section 13, Line 6, '134)". Appellants presume that this statement is intended to show where step "i." in claim 14 is found in Kikuchi. However, Appellants disagree that this referenced portion of Kikuchi or any other portion of Kikuchi shows each and every feature and relationship recited in step "i." in claim 14. For example, step "i." in claim 14 recites:

> i. the second one of the set of server computers extracting server-identifying data from the received cookie to retrieve the associated public key for the encrypted digital signature from the database for use in decrypting the digital signature for the received cookie and thereby authenticating the cookie.

Section 13 of Kikuchi discusses a Cookie verification part (14) which verifies whether there is alteration of the cookie. Section 13 also discusses a signature creation and verification part (15) which makes and verifies digital signatures for the cookies. However, again the verification parts (14, 15) are located on the same server (1) which created and sent the cookie to the client.

Nowhere does Kikuchi disclose or suggest that a different WWW server other than the one that generated the cookie is operative to decrypt digital signatures for received cookies. Further, nowhere does Kikuchi disclose or suggest the recited infrastructure that would even make this possible. For example, as explained previously, the cookies of Kikuchi do not include server-identifying data. Thus Kikuchi is not capable of extracting server-identifying data from the received cookie, so as to be able to retrieve the associated public key for the encrypted digital signature from the database for use in decrypting the digital signature for the received cookie. Kikuchi does not disclose or suggest a system that is capable of having a server authenticate a cookie generated by another server. Thus Kikuchi does not disclose or suggest step "i." of claim 14.

In addition the Actions have not shown where either Schneier or Devine discloses or suggests this step which is not disclosed or suggested in Kikuchi. Although Devine teaches that the system includes session data/cookie mapping to provide the identity of the user and any other "session-related information" (Figure 4, Column 14, lines 6-10), nowhere does Devine disclose or suggest that its described "cookie jar" server (32) or any other server places a unique server-identifier in the cookies. Further, nowhere does Devine disclose or suggest that any other information placed in a cookie may be used to identify a server that generated the cookie and/or be used to retrieve a public key associated with the server that generated the cookie.
Thus nowhere do Kikuchi, Schneier and Devine disclose or suggest extracting server-identifying data from the received cookie. Also, nowhere do Kikuchi, Schneier and Devine disclose or suggest extracting server-identifying data from the received cookie, so as to be able to retrieve the associated public key for the encrypted digital signature from a database for use in decrypting

the digital signature for the received cookie. Thus the Office has not established *prima facie* obviousness with respect to step "i." of claim 14.

The applied references do not disclose or suggest each of the features, relationships and steps recited in claim 14 and the Office has not established *prima facie* obviousness. In addition, as nothing in the cited art discloses or suggests the features, relationships, and steps that are specifically recited in the claim, and because there is no prior art teaching, suggestion or motivation cited for combining features of the cited references so as to produce Appellants' invention, it is respectfully submitted that claim 14 is allowable for these reasons. Therefore, it is respectfully submitted that the 35 U.S.C. § 103(a) rejection should be withdrawn. It follows that claims 15-16 which depend from claim 14 are likewise allowable.

Claim 15

Claim 15 depends from claim 12. The earlier Action admits that Kikuchi does not explicitly teach the recited feature of a "computer readable program code responsive to the restart of a one of the server computers and operative to request a replacement private key and an associated replacement public key". However, the Examiner states that he takes official notice as to the means to obtain a replacement key after restart. Appellants disagree.

The present evidence of record does not teach or suggest such features. The rejection relies on conclusory statements, not evidence of record. The Action's mere assertions do not constitute the required prior art evidence of record, and thus lack substantial evidence support. The determination of patentability must be based on evidence of record, not on unsubstantiated assertions under the guise of an Official notice (which is the present situation). As the evidence

of record does not support the rejection, the claims should be allowed. *In re Zurko*, supra. *In re Lee*, supra. MPEP § 2144.03.

Nowhere does Kikuchi disclose or suggest a server that ever requests a private key and associated public key. Also nowhere does Kikuchi disclose or suggest that a private key is only stored on the server in dynamic memory. In addition, nowhere does Kikuchi disclose or suggest storing a public key in a database. Thus whether or not volatile dynamic memory is well known in the art, nowhere does Kikuchi, Schneier, and Devine in view of volatile dynamic memory disclose or suggest a server that requests a replacement private key and an associated replacement public key in response to a restart. Further Kikuchi, Schneier, and Devine in view of volatile dynamic memory do not disclose or suggest as recited in claim 14 "storing the replacement public key in the database". Thus the Office has not established *prima facie* obviousness with respect to claim 14, and it is respectfully submitted the rejection should be reversed.

Claim 16

Claim 16 depends from claim 14. The Examiner acknowledged in the earlier Action that Kikuchi does not teach the features recited in claim 13 which recited similar subject matter as claim 14. However, the earlier Action states that "it would have been obvious . . . to implement '134 with the key lifecycle strategies as disclosed in Schneier." Appellants disagree.

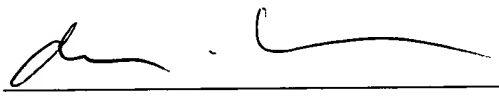
As discussed previously, Kikuchi does not disclose or suggest storing public keys in a database. Also Schneier does not provide a teaching, suggestion, or motivation to modify Kikuchi to include the recited database of public keys. Thus one of ordinary skill in the art

would not have been motivated to modify Kikuchi to perform the recited step of "deleting public keys in the database where such keys have been stored for longer than a predetermined elapsed time", because Kikuchi does not disclose or suggest having such a database. Thus, Appellants respectfully request that the 35 U.S.C. § 103(a) rejection of claim 16 be withdrawn.

CONCLUSION

Each of Appellants' pending claims specifically recites elements, features, relationships, and steps that are neither disclosed nor suggested in any of the applied prior art. Furthermore, the applied prior art is devoid of any teaching, suggestion, or motivation for producing the recited invention. For these reasons, it is respectfully submitted that all the pending claims are allowable.

Respectfully submitted,



Christopher L. Parmelee Reg. No. 42,980
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000

(viii) CLAIMS APPENDIX

11. A computer program product for use with a client-server computer network, the network comprising a set of server computers and a set of client computers, said computer program product comprising a computer usable medium having computer readable program code embodied in said medium for providing authentication of cookies, said computer program product comprising:

a. computer readable program code operative to enable one or more of the set of client computers to provide client-identifying data to one or more of the set of server computers,

b. computer readable program code operative to provide a unique server-identifier for each one of the set of server computers,

c. computer readable program code operative to enable each one of the set of server computers to request a private key and an associated public key from a public key encryption system,

d. computer readable program code operative to enable each one of the set of server computers to store the requested private key in a dynamic memory device on the server

computer, only,

e. computer readable program code operative to enable each one of the set of server computers to store the requested public key in a database available to the set of server computers, and to associate the stored public key requested by the server computer with the unique server-identifier for the server computer,

f. computer readable program code operative to enable each one of the set of server computers to generate cookies for one or more of the set of client computers, each generated cookie comprising data corresponding to the client-identifying data provided by the one or more of the set of client computers and comprising the value of the server-identifier assigned to the generating server,

g. computer readable program code operative to enable each one of the set of server computers to generate an encrypted digital signature for each generated cookie using the requested private key stored in dynamic memory on the server computer,

h. computer readable program code operative to enable each one of the set of server computers to forward cookies and their associated encrypted digital signatures to the client computers corresponding to the identifying data provided,

i. computer readable program code operative to enable each one of the set of server computers to receive cookies with encrypted digital signatures from one or more of the set of client computers, and

j. computer readable program code operative to enable each one of the set of server computers to extract server-identifying data from received cookies to retrieve associated public keys from the database for use in decrypting digital signatures for received cookies and thereby to authenticate the said cookies.

12. The computer program product of claim 11, further comprising computer readable program code responsive to the restart of a one of the server computers and operative to request a replacement private key and an associated replacement public key,

computer readable program code operative to cause the replacement private key to be stored in the dynamic memory of the server computer, and

computer readable program code operative to cause the replacement public key to be stored in the database.

13. The computer program product of claim 12, further comprising computer readable program code operative to cause the deletion of public keys in the database where such keys have been stored for longer than a predetermined elapsed time.

14. A method for providing authentication of cookies in a client-server computer network, the network comprising a set of server computers and a set of client computers, each one of the set of server computers having a unique server-identifier, the method comprising the following steps:

a. a first one of the set of client computers providing client-identifying data to a first one of the set of server computers,

b. the first one of the set of server computers requesting a private key and an associated public key from a public key encryption system,

c. the first one of the set of server computers storing the requested private key in a dynamic memory device; on the first server computer, only,

d. the first one of the set of server computers causing the requested public key to be stored in a database available to each one of the set of server computers, and to associate the stored public key with the unique server-identifier for the first one of the set of server computers,

e. the first one of the set of server computers generating a cookie for the first one of the set of client computers, the cookie comprising data corresponding to the client-identifying data provided by the first one of the set of client computers, and comprising

the value of the server-identifier for the first one of the set of server computers,

f. the first one of the set of server computers generating an encrypted digital signature for the cookie using the private key stored in dynamic memory of the first one of the set of server computers,

g. the first one of the set of server computers forwarding the cookie including the associated encrypted digital signature to the first one of the set of client computers,

h. the first one of the set of client computers communicating with a second one of the set of server computers, and in response, the second one of the set of server computers requesting and receiving the cookie including the encrypted digital signature from the first one of the set of client computers,

i. the second one of the set of server computers extracting server-identifying data from the received cookie to retrieve the associated public key for the encrypted digital signature from the database for use in decrypting the digital signature for the received cookie and thereby authenticating the cookie.

15. The method of claim 14 comprising the further steps of:

the first one of the set of server computers requesting a replacement private key and an associated replacement public key in response to a restart,

storing the replacement private key in the dynamic memory of the server computer, and

storing the replacement public key in the database.

16. The method of claim 14 comprising the further step of deleting public keys in the database where such keys have been stored for longer than a predetermined elapsed time.

(ix) EVIDENCE APPENDIX

(None)

(x) RELATED PROCEEDINGS APPENDIX

(None)